ソーシャル・ルータの提案

櫻井　孝一[†]　新城　靖[††]　佐藤　聡[††]
中井　央[†††]　板野　肯三[††]

1. はじめに

現在、Facebook や Twitter に代表される SNS(Social Network Service) は重要なインフラとなっている。従来の SNS では中央サーバにデータは蓄積される。データが蓄積される中央サーバは信頼出来るとは限らない。SNS の中央サーバが攻撃され、蓄積されるユーザのプライバシや機密情報が漏れる危険性がある。

中央のサーバを介さずに SNS メンバ同士でネットワークを通したアプリケーションを利用したい要望がある。この場合、DNS やルータのアクセス制御リストを設定すれば可能ではあるが、それには高いスキルが必要であり、手間も大きい。また、SNS のメンバ以外からもアクセス可能になるので、インターネットからの攻撃にさらされてしまうことがある。

このような問題を解決するために本研究では、SNS に特化した家庭用ルータを提案する。このルータをソーシャル・ルータと呼ぶ。ソーシャル・ルータは SNS メンバの PC 間の、中央サーバを経由しない、通信を容易にする。ソーシャル・ルータでは相手の PC をユーザ名で指定可能にする。ソーシャル・ルータでは SNS のユーザ ID と SNS グループ ID を用いてアクセス制御の設定を行えるようにする。本研究では、SNS メンバ同士で NFS でのファイル共有や talk などの LAN 用のアプリケーションを容易に利用できるようにする。

2. SNS における家庭用ルータと VPN の問題

家庭用ルータは簡単な設定でインターネットへアクセスできるように設計されている。家庭用ルータはルーティング以外に利用者への利便性を向上させる機能として、DHCP による IP アドレスの割当や DNS キャッシュサーバの機能を持っている、さらに、セキュリティを高める機能を持っている。家庭用のルータではパケットフィルタより外部のネットワークから LAN 内のネットワーク機器への TCP 接続を受け入れないように設定することが一般的である。その場合、外部からの接続を待ち受けるサーバアプリケーションやクライアントを LAN 内では実行することはできない。例えば SNS のユーザ間でファイルサーバを用いて、データを共有することを考える。この時、サーバを提供する側で外部からの接続を受け入れるためにルータのパケットフィルタの設定を変更し、SNS メンバに IP アドレスを通知する必要がある。このことは、1 章で述べたようにスキルと手間の問題がある。家庭用ルータには UPnP[2] によりパケットフィルタの設定や Dynamic DNS で IP アドレスの設定を自動化できるものもある。そうしたとしても、1 章で述べたように攻撃される問題がある。

VPN(Virtual Private Network) は LAN とネットワーク外の PC を暗号化通信でトンネリング接続し、ネットワーク外の PC を LAN 内の PC として通信できるようにする。VPN を用いることでルータのパケットフィルタをバイパスして外部 PC から通信を受け入れることができる。VPN ではすべての通信が許可されるので、SNS のメンバ間で利用するには問題がある。例えば SNS のメンバに悪意のあるメンバがいた場合、攻撃される可能性がある。

3. ソーシャル・ルータ

本研究で提案するソーシャル・ルータは家庭用ルータに次のようなソーシャル機能を追加したものである。

- 接続相手の PC を SNS ユーザ名を含むドメイン名で指定できる。
- SNS ユーザ ID と利用サービスによるアクセス制御を行うことができない。

3.1 SNS ユーザ名による PC 指定

本研究では SNS グループに所属するユーザ同士で通信する場合、ユーザ名で相手の PC を指定できるようにする。例えばユーザ名が Alice なら PC のアドレスは alice.socialrouter、ユーザ名が Bob なら PC の

† 筑波大学システム情報工学研究科
†† 筑波大学システム情報系
††† 筑波大学図書館情報メディア系

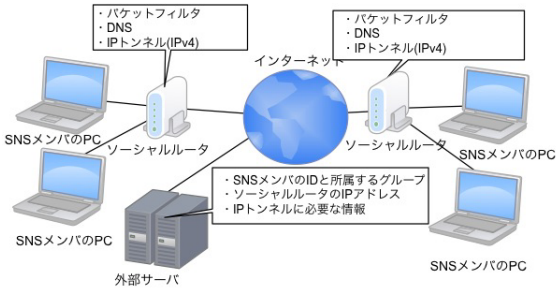

図 1 ソーシャル・ルータの外部サーバを用いた設定

アドレスは bob.socialrouter として付けることを可能にする。PC のアドレスは DNS(Domain Name Service) へ IPv4 は A レコードとして、IPv6 なら AAAA レコードで登録される。ユーザが複数の PC を持っている場合、サブドメインを利用して名前をつける。例えば alice-1.alice.socialrouter とすることができる。

3.2 SNS ユーザ ID によるアクセス制御

ソーシャル・ルータではパケットフィルタによるアクセス制御を、SNS のユーザ ID とグループ ID で行えるようにする。また、SNS メンバが利用できるサービスを限定する。たとえば NFS なら Linux のパケットフィルタの iptables では次のコマンドで設定できる。

```
iptables -A FORWARD -d alice.socialrouter -p tcp
-dport 111,1023,2049 -s bob.socialrouter
```

この例はクライアントとなる Bob の PC が、Alice の PC で動くサーバへ NFS でアクセスするために必要な通信ポートへアクセスを許可している。ポート番号 111、1023、2049 は NFS サーバで必要なものである。

3.3 IPv4 でのトネリング

家庭用ルータでは IPv4 の通信を行うには NAPT（Network Address Port Translation）を用いて一つの外部アドレスを複数の PC と共有することが一般的である。IPv4 で SNS メンバが NAPT を超えて通信するにはソーシャル・ルータ間に IP トンネルを構築し、通信を可能にする。IPv6 では IP トンネルを構築する必要はない。

4. OAuth を利用する SNS を対象とした実装

本研究では、Facebook や Twitter などの OAuth を用いている SNS を対象としてソーシャル・ルータを実装している。図 1 にその全体像を示す。

Facebook にはグループ機能があり、SNS メンバがグループ内で交流できる。本実装ではグループに属する SNS メンバの PC 間の通信を簡単に可能にする。

OAuth を用いてソーシャル・ルータを実現するためにはインターネット上に外部サーバが必要になる。外部サーバは SNS メンバを OAuth で認証すると各 SNS メンバの家庭にあるソーシャル・ルータに次のような情報を送信する。

- SNS メンバの ID と所属するグループ
- SNS メンバのソーシャル・ルータの IP アドレス
- IP トンネルに必要な情報（IPv4 のみ）

ソーシャル・ルータはこのような情報を受け取るとパケットフィルタを設定し、ローカルの DNS サーバに SNS メンバの PC を登録する。すると、グループに属する SNS メンバは他の SNS メンバと通信が可能になる。

5. 関 連 研 究

本研究の関連研究として Social VPN[1] がある。この研究は P2P-VPN という VPN のユーザ認証をソーシャルネットワークのアカウントを利用して行える。この Social VPN では XMPP(Extensible Messaging and Presence Protocol) に対応しているサービスのアカウントなら利用することができる。本研究で提案するソーシャル・ルータは、PC ではなくルータを利用している点が異なる。また、VPN のように PC の接続が全面的な開放ではなく特定のサービスのみアクセス可能にしている点も異なる。

6. ま と め

本研究では SNS 内のメンバ間の通信を容易にするソーシャル・ルータを提案した。ソーシャル・ルータでは DNS により、メンバの PC を簡単に指定でき、パケットフィルタを用いることでセキュリティを保つ。今後は実装を完成させ、多くの SNS メンバで利用した場合の動作を検証していく。

参 考 文 献

1) Renato J. Figueiredo, P. Oscar Boykin, Pierre St. Juste, and David Wolinsky. Social vpns: Integrating overlay and social networks for seamless p2p networking. *IEEE WETICE/COPS*, 2008.

2) Matthew Schmitz, Ulhas Warrier, and Prakash Iyer. Wanipconnection:1 service template version 1.01 for upnp™version 1.0. *UPnP Forum*, 2001.